CYCLIC COVERS OF THE PROJECTIVE LINE, THEIR JACOBIANS AND ENDOMORPHISMS

YURI G. ZARHIN

1. Introduction

As usual, $\mathbf{Z}, \mathbf{Q}, \mathbf{C}$ denote the ring of integers, the field of rational numbers and the field of complex numbers respectively. Let p be an odd prime. Recall that p is called a *Fermat prime* if $p = 2^{2^r} + 1$ for some positive integer r; e.g., $3, 5, 17, 257$ are Fermat prime.

Let us fix a primitive pth root of unity

$$\zeta_p \in \mathbf{C}.$$

Let $\mathbf{Q}(\zeta_p)$ be the pth cyclotomic field. It is well-known that $\mathbf{Q}(\zeta_p)$ is a CM-field. If p is a Fermat prime then the only CM-subfield of $\mathbf{Q}(\zeta_p)$ is $\mathbf{Q}(\zeta_p)$ itself, since the Galois group of $\mathbf{Q}(\zeta_p)/\mathbf{Q}$ is a cyclic 2-group, whose only element of order 2 acts as the complex conjugation. All other subfields of $\mathbf{Q}(\zeta_p)$ are totally real.

Let $f(x) \in \mathbf{C}[x]$ be a polynomial of degree $n \geq 4$ without multiple roots. Let $C_{f,p}$ be a smooth projective model of the smooth affine curve

$$y^p = f(x).$$

It is well-known ([6], pp. 401–402, [18], Prop. 1 on p. 3359, [13], p. 148) that the genus $g(C_{f,p})$ of $C_{f,p}$ is $(p-1)(n-1)/2$ if p does not divide n and $(p-1)(n-2)/2$ if it does. The map

$$(x, y) \mapsto (x, \zeta_p y)$$

gives rise to a non-trivial birational autmorphism

$$\delta_p : C_{f,p} \to C_{f,p}$$

of period p.

Let $J^{(f,p)} = J(C_{f,p})$ be the jacobian of $C_{f,p}$; it is an abelian variety, whose dimension equals $g(C_{f,p})$. We write $\mathrm{End}(J^{(f,p)})$ for the ring of endomorphisms of $J^{(f,p)}$. By functoriality, δ_p induces an automorphism of $J^{(f,p)}$ which we still denote by δ_p; it is known ([13], p. 149, [14], p. 448)) that

$$\delta^{p-1} + \cdots + \delta_p + 1 = 0$$

in $\mathrm{End}(J^{(f,p)})$. This gives us an embeddding

$$\mathbf{Z}[\zeta_p] \cong \mathbf{Z}[\delta_p] \subset \mathrm{End}(J^{(f,p)})$$

([13], p. 149, [14], p. 448)).

Our main result is the following statement.

Partially supported by the NSF.

Theorem 1.1. *Let K be a subfield of $\mathbf{C}$ such that all the coefficients of $f(x)$ lie in K. Assume also that $f(x)$ is an irreducible polynomial in $K[x]$ of degree $n \ge 5$ and its Galois group over K is either the symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$. Then $\mathbf{Z}[\delta_p]$ is a maximal commutative subring in* $\mathrm{End}(J^{(f,p)})$.

If p is a a Fermat prime (e.g., $p = 3, 5, 17, 257$) then

$$\mathrm{End}(J^{(f,p)}) = \mathbf{Z}[\delta_p] \cong \mathbf{Z}[\zeta_p].$$

When $p = 3$ one may obtain an additional information about Hodge classes on self-products of the corresponding trigonal jacobian.

Theorem 1.2. *Let K be a subfield of $\mathbf{C}$ such that all the coefficients of $f(x)$ lie in K. Assume also that $f(x)$ is an irreducible polynomial in $K[x]$ of degree $n \ge 5$ and its Galois group over K is either the symmetric group $\mathbf{S}_n$ or the alternating group $\mathbf{A}_n$. If 3 does not divide $n-1$ then:*

(i) *Every Hodge class on each self-product of $J^{(f,3)}$ could be presented as a linear combination of products of divisor classes. In particular, the Hodge conjecture is true for each self-product of $J^{(f,3)}$.*

(ii) *If K is a number field containing $\sqrt{-3}$ then every Tate class on each self-product of $J^{(f,3)}$ could be presented as a linear combination of products of divisor classes. In particular, the Tate conjecture is true for each self-product of $J^{(f,3)}$.*

Example 1.3. The polynomial $x^n - x - 1 \in \mathbf{Q}[x]$ has Galois group $\mathbf{S}_n$ over $\mathbf{Q}$ ([15], p. 42). Therefore the ring of endomorphism (over $\mathbf{C}$) of the jacobian $J(C^{(n,3)})$ of the curve $C^{(n,3)} : y^3 = x^n - x - 1$ is $\mathbf{Z}[\zeta_3]$ if $n \ge 5$.

If $n = 3k - 1$ for some integer $k \ge 2$ then all Hodge classes on each self-products of $J(C^{(n,3)})$ could be presented as linear combinations of products of divisor classes. In particular, the Hodge conjecture is true for all these self-products. Notice that $J(C^{(n,3)})$ is an abelian variety defined over $\mathbf{Q}$ of dimension $n - 1 = 3k - 2$.

Remarks 1.4. (i) If $f(x) \in K[x]$ then the curve $C_{f,p}$ and its jacobian $J^{(f,p)}$ are defined over K. Let $K_a \subset \mathbf{C}$ be the algebraic closure of K. Clearly, all endomorphisms of $J^{(f,p)}$ are defined over K_a. This implies that in order to prove Theorem 1.1, it suffices to check that $\mathbf{Z}[\delta_p]$ is a maximal commutative subring in the ring of K_a-endomorphisms of $J^{(f,p)}$ or equivalently, that $\mathbf{Q}[\delta_p]$ is a maximal commutative $\mathbf{Q}$-subalgebra in the algebra of K_a-endomorphisms of $J^{(f,p)}$.

(ii) Assume that $p = 3$ and $\mathbf{Z}[\delta_3] = \mathrm{End}(J^{(f,3)})$. The endomorphism algebra $\mathrm{End}^0(J^{(f,p)}) = \mathrm{End}(J^{(f,p)}) \otimes \mathbf{Q}$ is the imaginary quadratic field $\mathbf{Q}(\delta_3) \cong \mathbf{Q}(\sqrt{-3})$.

There are exactly two embeddings

$$\sigma, \bar{\sigma} : \mathbf{Q}(\delta_3) \hookrightarrow K_a \subset \mathbf{C}$$

and they are complex-conjugate. We have

$$\mathbf{Q}(\delta_3) \otimes_{\mathbf{Q}} \mathbf{C} = \mathbf{C} \oplus \mathbf{C}.$$

By functoriality, $\mathbf{Q}(\delta_3)$ acts on the $\mathbf{C}$-vector space $H^{1,0}(J^{(f,3)}) = \Omega^1(J^{(f,3)})$ of differentials of the fist kind. This action gives rise to a splitting of the $\mathbf{Q}(\delta_3) \otimes_{\mathbf{Q}} \mathbf{C} = \mathbf{C} \oplus \mathbf{C}$-module

$$H^{1,0}(J^{(f,3)}) = H^{1,0}_{\sigma} \oplus H^{1,0}_{\bar{\sigma}}.$$

The dimensions $n_\sigma := \dim_{\mathbf{C}}(H^{1,0}_\sigma)$ and $n_{\bar\sigma} := \dim_{\mathbf{C}}(H^{1,0}_{\bar\sigma})$ are called the *multiplicities* of σ and $\bar\sigma$ respectively. Clearly, n_σ (resp. $n_{\bar\sigma}$) coincides with the multiplicity of the eigenvalue $\sigma(\delta_3)$ (resp. $\bar\sigma(\delta_3)$) of the induced $\mathbf{C}$-linear operator

$$\delta_3^* : \Omega^1(J^{(f,3)}) \to \Omega^1(J^{(f,3)}).$$

By a theorem of Ribet ([11], Th. 3 on p. 526), if the multiplicities n_σ and $n_{\bar\sigma}$ are *relatively prime* and $\mathrm{End}^0(J^{(f,3)}) = \mathbf{Q}(\delta_3)$ then every Hodge class on each self-product of $J^{(f,3)}$ could be presented as a linear combination of products of divisor classes. Therefore, the assertion (i) of Theorem 1.2 would follow from Theorem 1.1 (with $p = 3$) if we know that the multiplicities n_σ and $n_{\bar\sigma}$ are relatively prime while 3 does not divide $n - 1$.

(iii) One may easily check that n_σ (resp. $n_{\bar\sigma}$) coincides with the multiplicity of the eigenvalue $\sigma(\delta_3)$ (resp. $\bar\sigma(\delta_3)$) of the induced $\mathbf{C}$-linear operator

$$\delta_3^* : \Omega^1(C_{(f,3)}) \to \Omega^1(C_{(f,3)}).$$

2. Permutation groups and permutation modules

Let B be a finite set consisting of $n \geq 5$ elements. We write $\mathrm{Perm}(B)$ for the group of permutations of B. A choice of ordering on B gives rise to an isomorphism

$$\mathrm{Perm}(S) \cong \mathbf{S}_n.$$

We write $\mathrm{Alt}(B)$ for the only subgroup in $\mathrm{Perm}(B)$ of index 2. Clearly, $\mathrm{Alt}(B)$ is normal and isomorphic to the alternating group $\mathbf{A}_n$. It is well-known that $\mathrm{Alt}(B)$ is a simple non-abelian group of order $n!/2$. Let G be a subgroup of $\mathrm{Perm}(B)$.

Let $\mathbf{F}$ be a field. We write $\mathbf{F}^B$ for the n-dimensional $\mathbf{F}$-vector space of maps $h : B \to F$. The space $\mathbf{F}^B$ is provided with a natural action of $\mathrm{Perm}(B)$ defined as follows. Each $s \in \mathrm{Perm}(B)$ sends a map $h : B \to \mathbf{F}_2$ into $sh : b \mapsto h(s^{-1}(b))$. The permutation module $\mathbf{F}^B$ contains the $\mathrm{Perm}(B)$-stable hyperplane

$$(\mathbf{F}^B)^0 = \{h : B \to \mathbf{F} \mid \sum_{b\in B} h(b) = 0\}$$

and the $\mathrm{Perm}(B)$-invariant line $\mathbf{F} \cdot 1_B$ where 1_B is the constant function 1. The quotient $\mathbf{F}^B/(\mathbf{F}^B)^0$ is a trivial 1-dimensional $\mathrm{Perm}(B)$-module.

Clearly, $(\mathbf{F}^B)^0$ contains $\mathbf{F} \cdot 1_B$ if and only if $\mathrm{char}(\mathbf{F})$ divides n. If this is *not* the case then there is a $\mathrm{Perm}(B)$-invariant splitting

$$\mathbf{F}^B = (\mathbf{F}^B)^0 \oplus \mathbf{F} \cdot 1_B.$$

Clearly, $\mathbf{F}^B$ and $(\mathbf{F}^B)^0$ carry natural structures of G-modules. Their (Brauer) characters depend only on characteristic of F.

Let us consider the case of $F = \mathbf{Q}$. Then the character of $\mathbf{Q}^B$ sends each $g \in G$ into the number of fixed points of g ([16], ex. 2.2,p.12); it takes on values in $\mathbf{Z}$ and called the *permutation character* of B. Let us denote by $\chi = \chi_B : G \to \mathbf{Q}$ the character of $(\mathbf{Q}^B)^0$.

It is known that the $\mathbf{Q}[G]$-module $(\mathbf{Q}^B)^0$ is absolutely simple if and only if G acts doubly transitively on B ([16], ex. 2.6, p. 17). Clearly, $1+\chi$ is the permutation character. In particular, χ also takes on values in $\mathbf{Z}$.

Now, let us consider the case of $\mathbf{F} = \mathbf{F}_p$.

If $p \mid n$ then let us define the $\mathrm{Perm}(B)$-module

$$(\mathbf{F}_p^B)^{00} := (\mathbf{F}_p^B)^0/(\mathbf{F}_p \cdot 1_B).$$

If p does not divide n then let us put

$$(\mathbf{F}_p^B)^{00} := (\mathbf{F}_p^B)^0.$$

Remark 2.1. Clearly, $\dim_{\mathbf{F}_p}((\mathbf{F}_p^B)^{00}) = n-1$ if n is not divisible by p and $\dim_{\mathbf{F}_p}((\mathbf{F}_p^B)^{00}) = n-2$ if $p \mid n$. In both cases $(\mathbf{F}_p^B)^{00}$ is a faithful G-module. One may easily check that if the $\mathbf{F}_p[G]$-module $(\mathbf{F}_p^B)^{00}$ is absolutely simple then the $\mathbf{Q}[G]$-module $(\mathbf{Q}^B)^0$ is also absolutely simple and therefore G acts doubly transitively on B.

Let $G^{(p)}$ be the set of p-regular elements of G. Clearly, the Brauer character of the G-module $\mathbf{F}_p^B$ coincides with the restriction of $1+\chi_B$ to $G^{(p)}$. This implies easily that the Brauer character of the G-module $(\mathbf{F}_p^B)^0$ coincides with the restriction of of χ_B to $G^{(p)}$.

Remark 2.2. Let us denote by $\phi_B = \phi$ the Brauer character of the G-module $(\mathbf{F}_p^B)^{00}$. One may easily check that ϕ_B coincides with the restriction of χ_B to $G^{(p)}$ if p does not divide n and with the restriction of $\phi_B - 1$ to $G^{(p)}$ if $p \mid n$. In both cases ϕ_B takes on values in $\mathbf{Z}$.

Example 2.3. Suppose $n = p = 5$ and $G = \mathrm{Alt}(B) \cong \mathbf{A}_5$. Then in the notations of [1], p. 2 and [5], p. 2 $\chi_B = 1 + \chi_4$ and the restriction of $\phi_B - 1 = \chi_4 - 1$ to $G^{(5)}$ coincides with absolutely irreducible Brauer character φ_2. This implies that the $\mathrm{Alt}(B)$-module $(\mathbf{F}_p^B)^{00}$ is absolutely simple.

The following elementary assertion is based on Lemma 7.1 on p. 52 of [12] and Th. 9.2 on p. 145 of [4]. (The case of $p = 2$ is Lemma 5.1 of [20]).

Lemma 2.4. *Assume that G acts doubly transitively on B. If p does not divide n then $\mathrm{End}_G((\mathbf{F}_p^B)^0) = \mathbf{F}_p$. In particular, if the G-module $(\mathbf{F}_p^B)^0$ is semisimple then it is absolutely simple.*

Proof. It suffices to check that $\dim_{\mathbf{F}_p}(\mathrm{End}_G((\mathbf{F}_p^B)^0)) \le 1$. Itn order to do that, recall that the double transitivity implies that $\dim_{\mathbf{F}_p}(\mathrm{End}_G((\mathbf{F}_p^B))) = 2$ (Lemma 7.1 on p. 52 of [12]). Now the desired inequality follows easily from the existence of the G-invariant splitting

$$\mathbf{F}_p^B = (\mathbf{F}_p^B)^0 \oplus \mathbf{F}_p \cdot 1_B.$$

□

Remark 2.5. Assume that $n = \#(B)$ is divisible by p. Let us choose $b \in B$ and let $G' := G_b$ be the stabilizer of b in G and $B' = B \setminus \{b\}$. Then $n' = \#(B') = n-1$ is not divisible by p and there is a canonical isomorphism of G'-modules

$$(\mathbf{F}_p^{B'})^{00} \cong (\mathbf{F}_p^B)^{00}$$

defined as follows. First, there is a natural G'-equivariant embedding $\mathbf{F}_p^{B'} \subset \mathbf{F}_p^B$ which could be obtained by extending each $h : B' \to \mathbf{F}_p$ to B by letting $h(b) = 0$. Second, this embedding identifies $(\mathbf{F}_p^{B'})^0$ with a hyperplane of $(\mathbf{F}_p^B)^0$ which does not contain 1_B. Now the composition

$$(\mathbf{F}_p^{B'})^{00} = (\mathbf{F}_p^{B'})^0 \subset (\mathbf{F}_p^B)^0 \to (\mathbf{F}_p^B)^0/(\mathbf{F}_p \cdot 1_B) = (\mathbf{F}_p^B)^{00}$$

gives us the desired isomorphism. This implies that if the G_b-module $(\mathbf{F}_p^{B'})^{00}$ is absolutely simple then the G-module $(\mathbf{F}_p^B)^{00}$ is also absolutely simple.

For example, if $G = \mathrm{Perm}(B)$ (resp. $\mathrm{Alt}(B)$) then $G_b = \mathrm{Perm}(B')$ (resp. $\mathrm{Alt}(B')$) and therefore the $\mathrm{Perm}(B')$-modules (resp. $\mathrm{Alt}(B')$-modules $(\mathbf{F}_p^B)^{00}$ and $(\mathbf{F}_p^{B'})^{00}$ are isomorphic. We use this observation in order to prove the following statement.

The following assertion goes back to Dickson.

Lemma 2.6. *Assume that $G = \mathrm{Perm}(B)$ or $\mathrm{Alt}(B)$. Then the G-module $(\mathbf{F}_p^B)^{00}$ is absolutely simple.*

Proof. In light of Example 2.3, we may assume that $(n, p) \neq (5, 5)$. In light of Remark 2.5 we may assume that p does not divide n and therefore

$$(\mathbf{F}_p^B)^{00} = (\mathbf{F}_p^B)^0.$$

The natural representation of $\mathrm{Perm}(B) = \mathbf{S}_n$ in $(\mathbf{F}_p^B)^0$ is irreducible ([3], Th. 5.2 on p. 133).

Since $\mathrm{Alt}(B)$ is normal in $\mathrm{Perm}(B)$, the $\mathrm{Alt}(B)$-module $(\mathbf{F}_p^B)^0$ is semisimple, thanks to Clifford's theorem ([2], §49, Th. 49.2). Since $n \geq 5$, the action of $\mathrm{Alt}(B) \cong \mathbf{A}_n$ on $B \cong \{1, \cdots, n\}$ is doubly transitive. Applying Lemma 2.4, we conclude that the $\mathrm{Alt}(B)$-module $(\mathbf{F}_p^{\mathfrak{R}_f})^0$ is absolutely simple. (See also [19].) □

3. Cyclic covers and jacobians

Throughout this paper we fix a prime p and assume that K is a field of characteristic zero. We fix its algebraic closure K_a and write $\mathrm{Gal}(K)$ for the absolute Galois group $\mathrm{Aut}(K_a/K)$. We also fix in K_a a primitive pth root of unity ζ.

Let $f(x) \in K[x]$ be a separable polynomial of degree $n \geq 4$. We write $\mathfrak{R}_f$ for the set of its roots and denote by $L = L_f = K(\mathfrak{R}_f) \subset K_a$ the corresponding splitting field. As usual, the Galois group $\mathrm{Gal}(L/K)$ is called the Galois group of f and denoted by $\mathrm{Gal}(f)$. Clearly, $\mathrm{Gal}(f)$ permutes elements of $\mathfrak{R}_f$ and the natural map of $\mathrm{Gal}(f)$ into the group $\mathrm{Perm}(\mathfrak{R}_f)$ of all permutations of $\mathfrak{R}_f$ is an embedding. We will identify $\mathrm{Gal}(f)$ with its image and consider it as a permutation group of $\mathfrak{R}_f$. Clearly, $\mathrm{Gal}(f)$ is transitive if and only if f is irreducible in $K[x]$. Therefore the $\mathrm{Gal}(f)$-module $(\mathbf{F}_p^{\mathfrak{R}_f})^{00}$ is defined. The canonical surjection

$$\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(f)$$

provides $(\mathbf{F}_p^{\mathfrak{R}_f})^{00}$ with canonical structure of the $\mathrm{Gal}(K)$-module via the composition

$$\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f) \subset \mathrm{Aut}((\mathbf{F}_p^{\mathfrak{R}_f})^{00}).$$

Let us put

$$V_{f,p} = (\mathbf{F}_p^{\mathfrak{R}_f})^{00}.$$

Let $C = C_{f,p}$ be the smooth projective model of the smooth affine K-curve

$$y^p = f(x).$$

So, C is a smooth projective curve defined over K. The rational function $x \in K(C)$ defined a finite cover $\pi : C \to \mathbf{P}^1$ of degree p. Let $B' \subset C(K_a)$ be the set of ramification points. Clearly, the restriction of π to B' is an *injective* map

$\pi : B' \hookrightarrow \mathbf{P}^1(K_a)$, whose image is the disjoint union of ∞ and $\mathfrak{R}_f$ if p does *not* divide $\deg(f)$ and just $\mathfrak{R}_f$ if it does. We write

$$B = \pi^{-1}(\mathfrak{R}_f) = \{(\alpha, 0) \mid \alpha \in \mathfrak{R}_f\} \subset B' \subset C(K_a).$$

Clearly, π is ramified at each point of B with ramification index p. We have $B' = B$ if and only if n is divisible by p. If n is not divisible by p then B' is the disjoint union of B and a single point $\infty' := \pi^{-1}(\infty)$; in addition, the ramification index of π at $\pi^{-1}(\infty)$ is also p. If p does divide n then $\pi^{-1}(\infty)$ consists of p unramified points denoted by $\infty_1, \dots, \infty_p$. This implies that the inverse image $\pi^*(n(\infty)) = n\pi^*(\infty)$ of the divisor $n(\infty)$ is always divisible by p in the divisor group of C. Using Hurwitz's formula, one may easily compute genus $g = g(C) = g(C_{p,f})$ of C ([6], pp. 401–402, [18], Prop. 1 on p. 3359, [13], p. 148). Namely, g is $(p-1)(n-1)/2$ if p does *not* divide p and $(p-1)(n-2)/2$ if it does. See §1 of [18] for an explicit description of a smooth complete model of C (when $n > p$).

Assume that K contains ζ. There is a non-trivial birational automorphism of C

$$\delta_p : (x, y) \mapsto (x, \zeta y).$$

Clearly, δ_p^p is the identity map and the set of fixed points of δ_p coincides with B'.

Let $J^{(f,p)} = J(C) = J(C_{f,p})$ be the jacobian of C. It is a g-dimensional abelian variety defined over K and one may view δ_p as an element of

$$\mathrm{Aut}(C) \subset \mathrm{Aut}(J(C)) \subset \mathrm{End}(J(C))$$

such that

$$\delta_p \neq \mathrm{Id}, \quad \delta_p^p = \mathrm{Id}$$

where Id is the identity endomorphism of $J(C)$. Here $\mathrm{End}(J(C))$ stands for the ring of all K_a-endomorphisms of $J(C)$. As usual, we write $\mathrm{End}^0(J(C)) = \mathrm{End}^0(J^{(f,p)})$ for the corresponding $\mathbf{Q}$-algebra $\mathrm{End}(J(C)) \otimes \mathbf{Q}$.

Lemma 3.1. $\mathrm{Id} + \delta_p + \cdots + \delta_p^{p-1} = 0$ *in* $\mathrm{End}(J(C))$. *Therefore the subring* $\mathbf{Z}[\delta_p] \subset \mathrm{End}(J(C))$ *is isomorphic to the ring* $\mathbf{Z}[\zeta_p]$ *of integers in the pth cyclotomic field* $\mathbf{Q}(\zeta_p)$. *The* $\mathbf{Q}$*-subalgebra*

$$\mathbf{Q}[\delta_p] \subset \mathrm{End}^0(J(C)) = \mathrm{End}^0(J^{(f,p)})$$

is isomorphic to $\mathbf{Q}(\zeta_p)$.

Proof. See [13], p. 149, [14], p. 448. □

Remarks 3.2. (i) Assume that p is odd and $n = \deg(f)$ is divisible by p say, $n = pm$ for some positive integer m. Then $n \geq 5$.

Let $\alpha \in K_a$ be a root of f and $K_1 = K(\alpha)$ be the corresponding subfield of K_a. We have

$$f(x) = (x - \alpha) f_1(x)$$

with $f_1(x) \in K_1[x]$. Clearly, $f_1(x)$ is a separable polynomial over K_1 of odd degree $pm - 1 = n - 1 \geq 4$. It is also clear that the polynomials

$$h(x) = f_1(x + \alpha), h_1(x) = x^{n-1} h(1/x) \in K_1[x]$$

are separable of the same degree $pm - 1 = n - 1 \geq 4$.

The standard substitution

$$x_1 = 1/(x - \alpha), y_1 = y/(x - \alpha)^m$$

establishes a birational isomorphism between $C_{f,p}$ and a superelliptic curve

$$C_{h_1} : y_1^p = h_1(x_1)$$

(see [18], p. 3359). But $\deg(h_1) = pm - 1$ is *not* divisible by p. Clearly, this isomorphism commutes with the actions of δ_p. In particular, it induces an isomorphism of $\mathbf{Z}[\delta_p]$-modules $J^{(f,p)}(K_a)$ and $J^{(h_1,p)}(K_a)$ which commutes with the action of $\mathrm{Gal}(K_1)$.

(ii) Assume, in addition, that $f(x)$ is irreducible in $K[x]$ and $\mathrm{Gal}(f)$ acts s-transitively on $\mathfrak{R}_f$ for some positive integer $s \geq 2$. Then the Galois group $\mathrm{Gal}(h_1)$ of h_1 over K_1 acts $s-1$-transitively on the set $\mathfrak{R}_{h_1}$ of roots of h_1. In particular, $h_1(x)$ is irreducible in $K_1[x]$.

It is also clear that if $\mathrm{Gal}(f) = \mathbf{S}_n$ or $\mathbf{A}_n$ then $\mathrm{Gal}(h_1) = \mathbf{S}_{n-1}$ or $\mathbf{A}_{n-1}$ respectively.

Let us put $\eta = 1 - \delta_p$. Clearly, η divides p in $\mathbf{Z}[\delta_p] \cong \mathbf{Z}[\zeta_p]$, i.e., there exists $\eta' \in \mathbf{Z}[\delta_p]$ such that

$$\eta\eta' = \eta'\eta = p \in \mathbf{Z}[\delta_p].$$

By a theorem of Ribet [10] the $\mathbf{Z}_p$-Tate module $T_p(J^{(f,p)})$ is a free $\mathbf{Z}_p[\delta_p]$-module of rank $2g/(p-1) = n-1$ if p does not divide n and $n-2$ if p does. Let $J^{(f,p)}(\eta)$ be the kernel of η in $J^{(f,p)}(K_a)$. Clearly, $J^{(f,p)}(\eta)$ is killed by multiplication by p, i.e., it may be viewed as a $\mathbf{F}_p$-vector space. It follows from Ribet's theorem that

$$\dim_{\mathbf{F}_p} J^{(f,p)}(\eta) = \frac{2g}{p-1}.$$

In addition, $J^{(f,p)}(\eta)$ carries a natural structure of Galois module. Notice that

$$\eta'(J_p^{(f,p)}) \subset J^{(f,p)}(\eta)$$

where $J_p^{(f,p)}$ is the kernel of multiplication by p in $J^{(f,p)}(K_a)$.

Let Λ be the centralizer of δ_p in $\mathrm{End}(J^{(f,p)})$. Clearly, Λ commutes with η and η'. It is also clear that the subgroup $J^{(f,p)}(\eta)$ is Λ-stable. This observation leads to a natural homomorphism

$$\kappa : \Lambda \to \mathrm{End}_{\mathbf{F}_p}(J^{(f,p)}(\eta)).$$

I claim that its kernel coincides with $\eta\Lambda$. Indeed, assume that $u(J^{(f,p)}(\eta)) = \{0\}$ for some $u \in \Lambda$. This implies that $u\eta' = \eta' u$ kills $J_p^{(f,p)}$. This implies, in turn, that there exists $v \in \mathrm{End}(J^{(f,p)})$ such that

$$u\eta' = \eta' u = pv = vp.$$

Clearly, v commutes with η and therefore with $\delta_p = 1 - \eta$, i.e., $v \in \Lambda$. Since $p = \eta\eta' = \eta'\eta$,

$$u\eta' = v\eta\eta'$$

and therefore $u = v\eta$. On the other hand, it is clear that $\eta\Lambda = \Lambda\eta$ kills $J^{(f,p)}(\eta)$. Therefore the natural map

$$\Lambda/\eta\Lambda \to \mathrm{End}_{\mathbf{F}_p}(J^{(f,p)}(\eta))$$

is an embedding; further we will identify $\Lambda/\eta\Lambda$ with its image in $\mathrm{End}_{\mathbf{F}_p}(J^{(f,p)}(\eta))$.

Theorem 3.3 (Prop. 6.2 in [13], Prop. 3.2 in [14])**.** *There is a canonical isomorphism of the* $\mathrm{Gal}(K)$*-modules*

$$J^{(f,p)}(\eta) \cong V_{f,p}.$$

Remark 3.4. Clearly, the natural homomorphism $\mathrm{Gal}(K) \to \mathrm{Aut}_{\mathbf{F}_p}(V_{f,p})$ coincides with the composition

$$\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f) \subset \mathrm{Aut}((\mathbf{F}_p^{\mathfrak{R}_f})^{00}) = \mathrm{Aut}_{\mathbf{F}_p}(V_{f,p}).$$

The following assertion is an immediate corollary of Lemma 2.6.

Lemma 3.5. *Assume that* $\mathrm{Gal}(f) = \mathbf{S}_n$ *or* $\mathbf{A}_n$. *If* $n \ge 5$ *then the* $\mathrm{Gal}(f)$*-module* $V_{f,p}$ *is absolutely simple.*

Theorem 3.6. *Assume that* $p > 2$ *and* $n \ge 4$. *Let* $\Lambda_{\mathbf{Q}} = \Lambda \otimes \mathbf{Q}$ *be the centralizer of* $\mathbf{Q}(\delta_p)$ *in* $\mathrm{End}^0(J^{(f,p)})$. *Then* $\Lambda_{\mathbf{Q}}$ *could not be a central simple* $\mathbf{Q}(\delta_p)$*-algebra of dimension* $(2g/(p-1))^2$ *where* g *is genus of* $C_{f,p}$.

Proof. Assume that $\Lambda_{\mathbf{Q}}$ is a central simple $\mathbf{Q}(\delta_p)$-algebra of dimension $(2g/(p-1))^2$. We need to arrive to a contradiction. We start with the following statement.

Lemma 3.7. *Assume that* $\Lambda_{\mathbf{Q}}$ *is a central simple* $\mathbf{Q}(\delta_p)$*-algebra of dimension* $(2g/(p-1))^2$. *Then there exist a* $(p-1)/2$*-dimensional abelian variety* Z *over* K_a, *a positive integer* r, *an embedding*

$$\mathbf{Q}(\zeta_p) \cong \mathbf{Q}(\delta_p) \hookrightarrow \mathrm{End}^0(Z)$$

and an isogeny $\phi : Z^r \to J^{(f,p)}$ *such that the induced isomorphism*

$$\mathrm{Mat}_r(\mathrm{End}^0(Z)) = \mathrm{End}^0(Z^r) \cong \mathrm{End}^0(J^{(f,p)}), \quad u \mapsto \phi u \phi^{-1}$$

maps identically

$$\mathbf{Q}(\delta_p) \subset \mathrm{End}^0(Z) \subset \mathrm{Mat}_r(\mathrm{End}^0(Z)) = \mathrm{End}^0(Z^r)$$

onto

$$\mathbf{Q}(\delta_p) \subset \mathrm{End}^0(J^{(f,p)}).$$

(Here $\mathrm{End}^0(Z) \subset \mathrm{Mat}_r(\mathrm{End}^0(Z))$ *is the diagonal embedding.) In particular,* Z *and* $J^{(f,p)}$ *are abelian varieties of CM-type over* K_a.

Proof of Lemma 3.7. Clearly, there exist a positive integer r and a central division algebra H over $\mathbf{Q}(\delta_p) \cong \mathbf{Q}(\zeta_p)$ such that $\Lambda_{\mathbf{Q}} \cong \mathrm{Mat}_r(H)$. This imples that there exist an abelian variety Z over K_a with

$$\mathbf{Q}(\delta_p) \subset H \subset \mathrm{End}^0(Z)$$

and an isogeny $\phi : Z^r \to J^{(f,p)}$ such that the induced isomorphism $\mathrm{End}^0(Z^r) \cong \mathrm{End}^0(J^{(f,p)})$ maps identically

$$\mathbf{Q}(\delta_p) \subset \mathrm{End}^0(Z) \subset \mathrm{End}^0(Z^r)$$

onto $\mathbf{Q}(\delta_p) \subset \mathrm{End}^0(J^{(f,p)})$. We still have to check that

$$2\dim(Z) = p - 1.$$

In order to do that let us put $g' = g/r$. Then $\dim_{\mathbf{Q}(\delta_p)}(H) = (\frac{2g'}{p-1})^2$ and therefore $\dim_{\mathbf{Q}}(H) = \frac{(2g')^2}{p-1}$. Since H is a division algebra and $\mathrm{char}(K_a) = 0$, the number $\frac{(2g')^2}{p-1}$ must divide $2\dim(Z) = 2g'$. This means that $2g'$ divides $p-1$. On the other hand,

$$\mathbf{Q}(\delta_p) \subset H \subset \mathrm{End}^0(Z).$$

This implies that $p - 1 = [\mathbf{Q}(\delta_p) : \mathbf{Q}]$ divides $2\dim(Z)$ and therefore $2\dim(Z) = p - 1$. □

Now let us return to the proof of Theorem 3.6. Recall that $n \geq 4$. We write $\Omega^1(X)$ for the space of differentials of first kind for any smooth projective variety X over K_a. Clearly, ϕ induces an isomorphism $\phi^* : \Omega^1(J^{(f,p)}) \cong \Omega^1(Z^r) = \Omega^1(Z)^r$ which commutes with the natural actions of $\mathbf{Q}(\delta_p)$. Since $\dim(Z) = \frac{p-1}{2}$, we have $\dim_{K_a}(\Omega^1(Z)) = \frac{p-1}{2}$. Therefore, the induced K_a-linear automorphism

$$\delta_p^* : \Omega^1(Z) \to \Omega^1(Z)$$

has, at most, $\frac{p-1}{2}$ distinct eigenvalues. Clearly, the same is true for the action of δ_p in $\Omega^1(Z)^r$. Since ϕ commutes with δ_p, the induced K_a-linear automorphism

$$\delta_p^* : \Omega^1(J^{(f,p)}) \to \Omega^1(J^{(f,p)})$$

has, at most, $\frac{p-1}{2}$ distinct eigenvalues.

On the other hand, let P_0 be one of the δ_p-invariant points (i.e., a ramification point for π) of $C_{f,p}(K_a)$. Then

$$\tau : C_{f,p} \to J^{(f,p)}, \quad P \mapsto \mathrm{cl}((P) - (P_0))$$

is an embedding of K_a-algebraic varieties and it is well-known that the induced map

$$\tau^* : \Omega^1(J^{(f,p)}) \to \Omega^1(C_{f,p})$$

is a K_a-linear isomorphism obviously commuting with the actions of δ_p. (Here cl stands for the linear equivalence class.) This implies that δ_p has, at most, $\frac{p-1}{2}$ distinct eigenvalues in $\Omega^1(C_{f,p})$.

One may easily check that $\Omega^1(C_{f,p})$ contains differentials dx/y^i for all positive integers $i < p$ satisfying $ni \geq (p+1)$ if p does not divide n ([6], Th. 3 on p. 403; see also [18], Prop. 2 on p. 3359). Since $n \geq 4$ and $p \geq 3$, we have $ni \geq (p+1)$ for all i with $\frac{p-1}{2} \leq i \leq p-1$. Therefore the differentials $dx/y^i \in \Omega^1(C_{f,p})$ for all i with $\frac{p-1}{2} \leq i \leq p-1$; clearly, they all are eigenvectors of δ_p with eigenvalues ζ^{-i} respectively. (Recall that $\zeta \in K_a$ is a primitive pth root of unity and δ_p is defined in §1 by $(x, y) \mapsto (x, \zeta y)$.) Therefore δ_p has in $\Omega^1(C_{f,p})$, at least, $\frac{p+1}{2}$ distinct eigenvalues. Contradiction.

Now assume that p divides n. Then $n \geq 5$. By Remark 3.2, $C_{f,p}$ is birationally isomorphic over K_a to a curve $C_1 = C_{h_1,p} : y_1^p = h_1(x_1)$ where $h_1(x_1) \in K_a[x_1]$ is a separable polynomial of degree $n-1$; in addition, one may choose this isomorphism in such a way that it commutes with the actions of δ_p on $C_{f,p}$ and $C_{h_1,p}$. This implies that δ_p has, at most, $\frac{p-1}{2}$ distinct eigenvalues in $\Omega^1(C_{h_1,p})$.

On the other hand, $n - 1 \geq 4$ and $n - 1$ is not divisible by p. Recall that $\deg(h_1) = n - 1$. We conclude, as above, that for all i with $\frac{p-1}{2} \leq i \leq p-1$ the differentials $dx_1/y_1^i \in \Omega^1(C_{h_1,p})$. Now, the same arguments as in the case of p not dividing n lead to a contradiction. □

Theorem 3.8. *Suppose $n \geq 4$ and $p > 2$. Assume that $\mathbf{Q}(\delta_p)$ is a maximal commutative subalgebra in $\mathrm{End}^0(J^{(f,p)})$. Then:*

(i) *The center $\mathfrak{C}$ of $\mathrm{End}^0(J^{(f,p)})$ is a CM-subfield of $\mathbf{Q}(\delta_p)$;*
(ii) *If p is a Fermat prime then $\mathrm{End}^0(J^{(f,p)}) = \mathbf{Q}(\delta_p) \cong \mathbf{Q}(\zeta_p)$ and therefore $\mathrm{End}(J^{(f,p)}) = \mathbf{Z}[\delta_p] \cong \mathbf{Z}[\zeta_p]$.*

Proof. Clearly, $\mathfrak{C} \subset \mathbf{Q}(\delta_p)$. Since $\mathbf{Q}(\delta_p)$ is a CM-field, $\mathfrak{C}$ is either a totally real field or a CM-field. If p is a Fermat prime then each subfield of $\mathbf{Q}(\delta_p)$ (distinct from $\mathbf{Q}(\delta_p)$ itself) is totally real. Therefore, (ii) follows from (i).

In order to prove (i), let us assume that $\mathfrak{C}$ is totally real. We are going to arrive to a contradiction which proves (i). Replacing, if necessary, K by its subfield finitely generated over the rationals, we may assume that K (and therefore K_a) is isomorphic to a subfield of the field $\mathbf{C}$ of complex numbers. Since the center $\mathfrak{C}$ of $\mathrm{End}^0(J^{f,p})$ is totally real, the Hodge group of $J^{(f,p)}$ must be semisimple. This implies that the pair $(J^{(f,p)}, \mathbf{Q}(\delta_p))$ is of *Weil type* ([8]), i.e., $\mathbf{Q}(\delta_p)$ acts on $\Omega^1(J^{(f,p)})$ in such a way that for each embedding

$$\sigma : \mathbf{Q}(\delta_p) \hookrightarrow \mathbf{C}$$

the corresponding multiplicity

$$n_\sigma = \frac{\dim(J^{(f,p)})}{[\mathbf{Q}(\delta_p) : \mathbf{Q}]}.$$

Now assume that p does not divide n. We have

$$\frac{\dim(J^{(f,p)})}{[\mathbf{Q}(\delta_p) : \mathbf{Q}]} = \frac{g(C_{f,p})}{p-1} = \frac{(n-1)}{2}$$

and therefore

$$n_\sigma = \frac{(n-1)}{2}.$$

Since the multiplicity n_σ is always an integer, n is odd. Therefore $n \geq 5$. Let us consider the embedding σ which sends δ_p to ζ. Elementary calculations ([6], Th. 3 on p. 403) show that for all integers i with

$$0 \leq i \leq n-1-\frac{(n+1)}{p}$$

the differentials $x^i dx/y^{p-1} \in \Omega^1(C_{f,p})$; clearly, they constitute a set of K_a-linearly independent eigenvectors of δ_p with eigenvalue ζ. In light of the δ_p-equivariant isomorphism

$$\Omega^1(J^{(f,p)}) \to \Omega^1(C_{f,p}),$$

we conclude that

$$\frac{(n-1)}{2} = n_\sigma \geq [n-1-\frac{(n+1)}{p}] + 1.$$

This implies that $\frac{(n-1)}{2} > n-1-\frac{(n+1)}{p}$. It follows easily that $n < \frac{p+2}{p-2} \leq 5$ and therefore $n < 5$. This gives us the desired contradiction when p does not divide n.

Now assume that p divides n. Then $n \geq 5$ and $n-1 \geq 4$. Again, as in the proof of Theorem 3.6, the usage of Remark 3.2 allows us to apply the already proven case (when p does not divide $n-1$) to $C_{h_1,p}$ with $\deg(h_1) = n-1$. □

Remark 3.9. Let us keep the notations and assumptions of Theorem 3.8. Assume, in addition that $p = 3$. Then $\mathbf{Q}(\delta_3) = \mathbf{Q}(\zeta_3)$ is an imaginary quadratic field and there are exactly two embeddings $\mathbf{Q}(\delta_3) \hookrightarrow K_a$ which, of course, are complex-conjugate. In this case one could compute explicitly the corresponding multiplicities.

Indeed, first assume that 3 does not divide n. Then $n = 3k - e$ for some $k, e \in \mathbf{Z}$ with $3 > e > 0$. Since $n \geq 4 > 3$, we have $k \geq 2$. By Prop. 2 on p. 3359 of [18], the set

$$\{x^i dx/y, 0 \leq i < k-1; x^j dx/y^2, 0 \leq j < 2k-1-[\frac{2e}{3}]\}$$

is a basis of $\Omega^1(C_{(f,3)})$. It follows easily that it is an eigenbasis with respect to the action of δ_3. This implies easily that $\mathbf{Q}(\delta_3)$ acts on $\Omega^1(J^{(f,3)}) = \Omega^1(C_{(f,3)})$ with multiplicities $k-1$ and $2k-1-[\frac{2e}{3}]$.

Assume now that $n = 3k$ is divisible by 3. Then as in the proof of Theorem 3.6, the usage of Remark 3.2 allows us to reduce the calculation of multiplicities to the case of $C_{h_1,3}$ with $\deg(h_1) = n-1$. More precisely, we have $n = 3k$ and $n-1 = 3k-1$, i.e., $e = 1$ and $k \geq 2$. This implies that $\mathbf{Q}(\delta_3)$ acts on $\Omega^1(J^{(f,3)}) = \Omega^1(J^{(h_1,3)})$ with multiplicities $k-1$ and $2k-1$.

It follows that if $n = 3k$ or $n = 3k-1$ then

$$\dim(J^{(f,3)}) = 3k - 2$$

and the imaginary quadratic field $\mathbf{Q}(\delta_3)$ acts on $\Omega^1(J^{(f,3)})$ with *mutually prime* multiplicities $k-1$ and $2k-1$. Since $\mathbf{Q}(\delta_3)$ coincides with $\mathrm{End}^0(J^{(f,3)})$, a theorem of Ribet ([11], Th. 3 on p. 526) implies that the Hodge group of $J^{(f,3)}$ is *as large as possible*. More precisely, let $K' \subset K$ be a subfield which admits an embedding into $\mathbf{C}$ and such that $f(x) \subset K'[x]$ (such a subfield always exists). Then one may consider $C_{f,3}$ as a complex smooth projective curve and $J^{(f,3)}$ as a complex abelian variety, whose endomorphism algebra coincides with $\mathbf{Q}(\delta_3) \cong \mathbf{Q}(\zeta_3) = \mathbf{Q}(\sqrt{-3})$. Then the Hodge group of $J^{(f,3)}$ coincides with the corresponding unitary group of $H_1(J^{(f,3)}(\mathbf{C}), \mathbf{Q})$ over $\mathbf{Q}(\zeta_3)$. In particular, all Hodge classes on all self-products of $J^{(f,3)}$ could be presented as linear combinations of exterior products of divisor classes. As was pointed out in [7], pp. 572–573, the same arguments work also for Tate classes if say, K' is a number field and all endomorphisms of $J^{(f,3)}$ are defined over K'. (If $\sqrt{-3} \in K'$ then all endomorphisms of $J^{(f,3)}$ are defined over K' because $\mathrm{End}(J^{(f,3)}) = \mathbf{Z}[\delta_3]$ and δ_3 is defined over $K'(\zeta_3) = K'(\sqrt{-3})$.)

4. Representation theory

Definition 4.1. Let V be a vector space over a field F, let G be a group and $\rho : G \to \mathrm{Aut}_F(V)$ a linear representation of G in V. We say that the G-module V is *very simple* if it enjoys the following property:

If $R \subset \mathrm{End}_F(V)$ be an F-subalgebra containing the identity operator Id such that

$$\rho(\sigma) R \rho(\sigma)^{-1} \subset R \quad \forall \sigma \in G$$

then either $R = F \cdot \mathrm{Id}$ or $R = \mathrm{End}_F(V)$.

Remark 4.2. (i) Clearly, the G-module V is very simple if and only if the corresponding $\rho(G)$-module V is very simple. It is known ([21], Rem. 2.2(ii)) that a very simple module is absolutely simple.

(ii) If G' is a subgroup of G and the G'-module V is very simple then the G-module V is also very simple.

Theorem 4.3. *Suppose a field F, a positive integer N and a group H enjoy the following properties:*

- *F is either finite or algebraically closed;*
- *H is perfect, i.e., $H = [H, H]$;*
- *Each homomorphism from H to $\mathbf{S}_N$ is trivial;*
- *Let $N = ab$ be a factorization of N into a product of two positive integers a and b. Then either each homomorphism from H to $\mathrm{PGL}_a(F)$ is trivial or each homomorphism from H to $\mathrm{PGL}_b(F)$ is trivial.*

Then each absolutely simple H-module of F-dimension N is very simple. In other words, in dimension N the properties of absolute simplicity and supersimplicity over F are equivalent.

Proof. We may assume that $N > 1$. Let V be an absolutely simple H-module of F-dimension N. Let $R \subset \mathrm{End}_F(V)$ be an F-subalgebra containing the identity operator Id and such that

$$uRu^{-1} \subset R \quad \forall u \in H.$$

Clearly, V is a faithful R-module and

$$uRu^{-1} = R \quad \forall u \in H.$$

Step 1. By Lemma 7.4(i) of [21], V is a *semisimple* R-module.

Step 2. The R-module V is *isotypic*. Indeed, let us split the semisimple R-module V into the direct sum

$$V = V_1 \oplus \cdots \oplus V_r$$

of its isotypic components. Dimension arguments imply that $r \le \dim(V) = N$. It follows easily from the arguments of the previous step that for each isotypic component V_i its image sV_i is an isotypic R-submodule for each $s \in H$ and therefore is contained in some V_j. Similarly, $s^{-1}V_j$ is an isotypic submodule obviously containing V_i. Since V_i is the isotypic component, $s^{-1}V_j = V_i$ and therefore $sV_i = V_j$. This means that s permutes the V_i; since V is H-simple, H permutes them transitively. This gives rise to the homomorphism $H \to \mathbf{S}_r$ which must be trivial, since $r \le N$ and therefore $\mathbf{S}_r$ is a subgroup of $\mathbf{S}_N$. This means that $sV_i = V_i$ for all $s \in H$ and $V = V_i$ is isotypic.

Step 3. Since V is isotypic, there exist a simple R-module W and a positive integer d such that $V \cong W^d$. We have

$$d \cdot \dim(W) = \dim(V) = N.$$

Clearly, $\mathrm{End}_R(V)$ is isomorphic to the matrix algebra $\mathrm{Mat}_d(\mathrm{End}_R(W))$ of size d over $\mathrm{End}_R(W)$.

Let us put

$$k = \mathrm{End}_R(W).$$

Since W is simple, k is a finite-dimensional division algebra over F. Since F is either finite or algebraically closed, k must be a field. In addition, $k = F$ if F is algebraically closed and k is finite if F is finite. We have

$$\mathrm{End}_R(V) \cong \mathrm{Mat}_d(k).$$

Clearly, $\mathrm{End}_R(V) \subset \mathrm{End}_F(V)$ is stable under the adjoint action of H. This induces a homomorphism

$$\alpha : H \to \mathrm{Aut}_F(\mathrm{End}_R(V)) = \mathrm{Aut}_F(\mathrm{Mat}_d(k)).$$

Since k is the center of $\mathrm{Mat}_d(k)$, it is stable under the action of H, i.e., we get a homomorphism $H \to \mathrm{Aut}(k/F)$, which must be trivial, since H is perfect and $\mathrm{Aut}(k/F)$ is abelian. This implies that the center k of $\mathrm{End}_R(V)$ commutes with H. Since $\mathrm{End}_H(V) = F$, we have $k = F$. This implies that $\mathrm{End}_R(V) \cong \mathrm{Mat}_d(F)$ and

$$\alpha : H \to \mathrm{Aut}_F(\mathrm{Mat}_d(F)) = \mathrm{GL}(d, F)/F^* = \mathrm{PGL}_d(F)$$

is trivial if and only if $\mathrm{End}_R(V) \subset \mathrm{End}_H(V) = F \cdot \mathrm{Id}$. Since $\mathrm{End}_R(V) \cong \mathrm{Mat}_d(F)$, α is trivial if and only if $d = 1$, i.e. V is an absolutely simple R-module.

It follows from the Jacobson density theorem that $R \cong \mathrm{Mat}_m(F)$ with $dm = N$. This implies that α is trivial if and only if $R \cong \mathrm{Mat}_N(F)$, i.e., $R = \mathrm{End}_{\mathbf{F}}(V)$.

The adjoint action of H on R gives rise to a homomorphism

$$\beta : H \to \mathrm{Aut}_F(\mathrm{Mat}_m(F)) = \mathrm{PGL}_m(F).$$

Clearly, β is trivial if and only if R commutes with H, i.e. $R = F \cdot \mathrm{Id}$.

It follows that we are done if either α or β is trivial. Now one has only to recall that $N = dm$. □

Corollary 4.4. *Let p be a prime, V a vector space over $\mathbf{F}_p$ of finite dimension N. Let $H \subset \mathrm{Aut}(V)$ be a non-abelian simple group. Suppose that the H-module V is absolutely simple and H is not isomorphic to a subgroup of $\mathbf{S}_N$. Then the H-module V is very simple if one of the following conditions holds:*

(i) *N is a prime;*
(ii) *$N = 8$ or twice a prime. In addition, H is not isomorphic to $PSL_2(\mathbf{F}_p)$ and either H is not isomorphic to $\mathbf{A}_5$ or p is not congruent to ± 1 modulo 5;*
(iii) $\#(H) \geq ((p^{[\sqrt{N}]} - 1)^{[\sqrt{N}]})/(p-1)$
(iv) $\#(H) \geq (p^N - 1)/(p-1)$.

Proof. Let us split N into a product $N = ab$ of two positive integers a and b. In the case (i) either a or b is 1 and the target of the corresponding projective linear group $\mathrm{PGL}_1(\mathbf{F}_p) = \{1\}$. In the case (ii) either one of the factors is 1 and we are done or one of the factors is 2 and it suffices to check that each homomorphism from H to $\mathrm{PGL}_2(\mathbf{F}_p)$ is trivial. Since H is simple, each non-trivial homomorphism $\gamma : H \to \mathrm{PGL}_2(\mathbf{F}_p)$ is an injection, whose image lies in $\mathrm{PSL}_2(\mathbf{F}_p)$. In other words, $\gamma(H)$ is a subgroup of $\mathrm{PSL}_2(\mathbf{F}_p)$ isomorphic to H. Since H is not isomorphic to $\mathrm{PSL}_2(\mathbf{F}_p)$, the subgroup $\gamma(H)$ is proper and simple non-abelian. It is known ([17], Th. 6.25 on p. 412 and Th. 6.26 on p. 414) that each proper simple non-abelian subgroup of $\mathrm{PSL}_2(\mathbf{F}_p)$ is isomorphic to $\mathbf{A}_5$ and such a subgroup exists if and only if p is congruent to ± 1 modulo 5. This implies that such γ does not exist and settles the case (ii). In order to do the case (iii) notice that one of the factors say, a does not exceed $[\sqrt{N}]$. This implies easily that the order of $\mathrm{GL}_a(\mathbf{F}_p)$ does not exceed $((p^{[\sqrt{N}]} - 1)^{[\sqrt{N}]})$ and therefore the order of $\mathrm{PGL}_a(\mathbf{F}_p)$ does not exceed $((p^{[\sqrt{N}]} - 1)^{[\sqrt{N}]})/(p-1)$. Hence, the order of H is strictly greater than the order of $\mathrm{PGL}_a(\mathbf{F}_p)$ and therefore there are no injective homomorphisms from H to $\mathrm{PGL}_a(\mathbf{F}_p)$. Since H is simple, each homomorphism from H is either trivial or injective. This settles the case (iii). The case (iv) follows readily from the case (iii).

□

Corollary 4.5. *Suppose $n \ge 5$ is an integer, B is an n-element set. Suppose $p = 3$. Then the* $\mathrm{Alt}(B)$*-module* $(\mathbf{F}_3^B)^{00}$ *is very simple.*

Proof. By Lemma 2.6, $(\mathbf{F}_3^B)^{00}$ is absolutely simple and $N = \dim_{\mathbf{F}_3}((\mathbf{F}_3^B)^{00})$ is either $n-1$ or $n-2$. The group $\mathrm{Alt}(B) \cong \mathbf{A}_n$ is a simple non-abelian group, whose order $n!/2$ is greater than the order of $\mathbf{S}_{n-1}$ and the order of $\mathbf{S}_{n-2}$. Therefore each homomorphism from $\mathrm{Alt}(B)$ to $\mathbf{S}_N$ is trivial. On the other hand, one may easily check that

$$n!/2 > 3^{n-1}/2 > (3^N - 1)/(3-1)$$

for all $n \ge 5$. Now one has only to apply Corollary 4.4(iv) to $H = \mathrm{Alt}(B)$ and $p = 3$. □

Corollary 4.6. *Suppose $p > 3$ is a prime, $n \ge 8$ is a positive integer, B is an n-element set. Then the* $\mathrm{Alt}(B)$*-module* $(\mathbf{F}_p^B)^{00}$ *is very simple.*

Proof. Recall that $N = \dim_{\mathbf{F}_p}((\mathbf{F}_p^B)^{00}$ is either $n-1$ or $n-2$. In both cases

$$[\sqrt{N}] - 1 < [n/3].$$

Clearly, $\mathrm{Alt}(B) \cong \mathbf{A}_n$ is perfect and every homomorphism from $\mathrm{Alt}(B)$ to $\mathbf{S}_N$ is trivial.

We are going to deduce the Corollary from Theorem 4.3 applied to $F = \mathbf{F}_p$ and $H = \mathrm{Alt}(B)$. In order to do that let us consider a factorization $N = ab$ of N into a product of two positive integers a and b. We may assume that $a > 1, b > 1$ and say, $a \le b$. Then

$$a - 1 \le [\sqrt{N}] - 1 < [n/3].$$

Let

$$\alpha : \mathbf{A}_n \cong \mathrm{Alt}(B) \to \mathrm{PGL}_a(\mathbf{F}_p)$$

be a group homomorphism. We need to prove that α is trivial. Let $\bar{\mathbf{F}}_p$ be an algebraic closure of $\mathbf{F}_p$. Since $\mathrm{PGL}_a(\mathbf{F}_p) \subset \mathrm{PGL}_a(\bar{\mathbf{F}}_p)$, it suffices to check that the composition

$$\mathbf{A}_n \cong \mathrm{Alt}(B) \to \mathrm{PGL}_a(\mathbf{F}_p) \subset \mathrm{PGL}_a(\bar{\mathbf{F}}_p)$$

which we continue denote by α, is trivial.

Let

$$\pi : \tilde{\mathbf{A}}_n \twoheadrightarrow \mathbf{A}_n$$

be the universal central extension of the perfect group $\mathbf{A}_n$. It is well-known that $\tilde{\mathbf{A}}_n$ is perfect and the kernel (Schur's multiplier) of π is a cyclic group of order 2, since $n \ge 8$. One could lift α to the homomorphism

$$\alpha' : \tilde{\mathbf{A}}_n \to \mathrm{GL}_a(\bar{\mathbf{F}}_p).$$

Clearly, α is trivial if and only if α' is trivial. In order to prove the triviality of α', let us put $m = [n/3]$ and notice that $\mathbf{A}_n$ contains a subgroup D isomorphic to $(\mathbf{Z}/3\mathbf{Z})^m$ (generated by disjoint 3-cycles). Let D' be a Sylow 3-subgroup in $\pi^{-1}(D)$. Clearly, π maps D' isomorphically onto D. Therefore, D' is a subgroup of $\tilde{\mathbf{A}}_n$ isomorphic to $(\mathbf{Z}/3\mathbf{Z})^m$.

Now, let us discuss the image and the kernel of α'. First, since $\tilde{\mathbf{A}}_n$ is perfect, its image lies in $\mathrm{SL}_a(\bar{\mathbf{F}}_p)$, i.e., one may view α' as a homomorphism from $\tilde{\mathbf{A}}_n$ to $\mathrm{SL}_a(\bar{\mathbf{F}}_p)$. Second, the only proper normal subgroup in $\tilde{\mathbf{A}}_n$ is the kernel of π. This implies that if α' is nontrivial then its kernel meets D' only at the identity element and therefore $\mathrm{SL}_a(\bar{\mathbf{F}}_p)$ contains the subgroup $\alpha'(D')$ isomorphic to $(\mathbf{Z}/3\mathbf{Z})^m$. Since

$p \ne 3$, the group $\alpha'(D')$ is conjugate to an elementary 3-group of diagonal matrices in $\mathrm{SL}_a(\bar{\mathbf{F}}_p)$. This implies that

$$m \le a - 1.$$

Since $m = [n/3]$, we get a contradiction which implies that our assumption of the nontriviality of α' was wrong. Hence α' is trivial and therefore α is also trivial. □

Theorem 4.7. *Suppose $n \ge 5$ is a positive integer, B is an n-element set, p is a prime. Then the* $\mathrm{Alt}(B)$*module* $(\mathbf{F}_p^B)^{00}$ *is very simple.*

Proof. The case of $p = 2$ was proven in [21], Ex. 7.2. The case of $p = 3$ was done in Corollary 4.5. So, we may assume that $p \ge 5$. In light of Corollary 4.6 we may assume that $n < 8$, i.e., $5 \le n \le 7$.

Assume that $n \ne p$. Then p does not divide n and $n - 1$ is either a prime or twice a prime. Therefore

$$N = \dim_{\mathbf{F}_p}((\mathbf{F}_p^B)^{00}) = n - 1$$

is either a prime or twice a prime. Now the very simplicity of $(\mathbf{F}_p^B)^{00}$ follows from the cases (i) and (ii) of Corollary 4.4.

Assume now that $n = p$. Then either $n = p = 5$ or $n = p = 7$. In both cases

$$N = \dim_{\mathbf{F}_p}((\mathbf{F}_p^B)^{00}) = n - 2$$

is a prime. Now the very simplicity of $(\mathbf{F}_p^B)^{00}$ follows from Corollary 4.4(i).

□

5. Jacobians and endomorphisms

Recall that K is a field of characteristic zero, $f(x) \in K[x]$ is a polynomial of degree $n \ge 5$ without multiple roots, $\mathfrak{R}_f \subset K_a$ the set of its roots, $K(\mathfrak{R}_f)$ its splitting field,

$$\mathrm{Gal}(f) = \mathrm{Gal}(K(\mathfrak{R}_f)/K) \subset \mathrm{Perm}(\mathfrak{R}_f).$$

Remark 5.1. Assume that $\mathrm{Gal}(f) = \mathrm{Perm}(\mathfrak{R}_f)$ or $\mathrm{Alt}(\mathfrak{R}_f)$. Taking into account that $\mathrm{Alt}(\mathfrak{R}_f)$ is non-abelian simple, $\mathrm{Perm}(\mathfrak{R}_f)/\mathrm{Alt}(\mathfrak{R}_f) \cong \mathbf{Z}/2\mathbf{Z}$ and $K(\zeta)/K$ is abelian, we conclude that the Galois group of f over $K(\zeta)$ is also either $\mathrm{Perm}(\mathfrak{R}_f)$ or $\mathrm{Alt}(\mathfrak{R}_f)$. In particular, f remains irreducible over $K(\zeta)$. So, in the course of the proof of main results from Introduction we may assume that $\zeta \in K$.

Theorem 5.2. *Let p be an odd prime and $\zeta \in K$. If the* $\mathrm{Gal}(f)$*-module* $(\mathbf{F}_p^{\mathfrak{R}_f})^{00}$ *is very simple then $\mathbf{Q}(\delta_p)$ coincides with its own centralizer in* $\mathrm{End}^0(J^{(f,p)})$ *and the center of* $\mathrm{End}^0(J^{(f,p)})$ *is a CM-subfield of $\mathbf{Q}(\delta_p)$. In particular, if p is a Fermat prime then* $\mathrm{End}^0(J^{(f,p)}) = \mathbf{Q}(\delta_p)$ *and* $\mathrm{End}(J^{(f,p)}) = \mathbf{Z}[\delta_p]$.

Combining Theorems 5.2, Remark 5.1, Theorem 4.7 and Remark 4.2(ii), we obtain the following statement.

Corollary 5.3. *Let p be an odd prime. If $f(x) \in K[x]$ is an irreducible polynomial of degree $n \ge 5$ and* $\mathrm{Gal}(f) = \mathbf{S}_n$ *or* $\mathbf{A}_n$ *then $\mathbf{Q}(\delta_p)$ is a maximal commutative subalgebra in* $\mathrm{End}^0(J^{(f,p)})$ *and the center of* $\mathrm{End}^0(J^{(f,p)})$ *is a CM-subfield of* $\mathbf{Q}(\delta_p)$. *In particular, if p is a Fermat prime then* $\mathrm{End}^0(J^{(f,p)}) = \mathbf{Q}(\delta_p)$ *and* $\mathrm{End}(J^{(f,p)}) = \mathbf{Z}[\delta_p]$.

Proof of Theorem 5.2. Recall that $J^{(f,p)}$ is a g-dimensional abelian variety defined over K.

Since $J^{(f,p)}$ is defined over K, one may associate with every $u \in \mathrm{End}(J^{(f,p)})$ and $\sigma \in \mathrm{Gal}(K)$ an endomorphism ${}^\sigma u \in \mathrm{End}(J^{(f,p)})$ such that

$$ {}^\sigma u(x) = \sigma u(\sigma^{-1}x) \quad \forall x \in J^{(f,p)}(K_a).$$

Let us consider the centralizer Λ of δ_p in $\mathrm{End}(J^{(f,p)})$. Since δ_p is defined over K, we have ${}^\sigma u \in \Lambda$ for all $u \in \Lambda$. Clearly, $\mathbf{Z}[\delta_p]$ sits in the center of Λ and the natural homomorphism

$$\Lambda \otimes \mathbf{Z}_p \to \mathrm{End}_{\mathbf{Z}_p[\delta_p]} T_p(J^{(f,p)})$$

is an embedding. Here $T_p(J^{(f,p)})$ is the $\mathbf{Z}_p$-Tate module of $J^{(f,p)}$ which is a free $\mathbf{Z}_p[\delta_p]$-module of rank $\frac{2g}{p-1}$. Notice that

$$J^{(f,p)}(\eta) = T_p(J^{(f,p)})/\eta T_p(J^{(f,p)}).$$

Recall also that (Theorem 3.3 and Remark 3.4)

$$J^{(f,p)}(\eta) = (\mathbf{F}_p^{\mathfrak{R}_f})^{00}$$

and $\mathrm{Gal}(K)$ acts on $(\mathbf{F}_p^{\mathfrak{R}_f})^{00}$ through

$$\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(f) \subset \mathrm{Perm}(\mathfrak{R}_f) \subset \mathrm{Aut}((\mathbf{F}_p^{\mathfrak{R}_f})^{00}).$$

Since the $\mathrm{Gal}(f)$-module $(\mathbf{F}_p^{\mathfrak{R}_f})^{00}$ is very simple, the $\mathrm{Gal}(K)$-module $J^{(f,p)}(\eta)$ is also very simple, thanks to Remark 4.2(i). On the other hand, if an endomorphism $u \in \Lambda$ kills $J^{(f,p)}(\eta) = \ker(1-\delta_p)$ then one may easily check that there exists a unique $v \in \mathrm{End}(J^{(f,p)})$ such that $u = v \cdot \eta$. In addition, $v \in \Lambda$. This implies that the natural map

$$\Lambda \otimes_{\mathbf{Z}[\delta_p]} \mathbf{Z}[\delta_p]/(\eta) \to \mathrm{End}_{\mathbf{F}_p}(J^{(f,p)}(\eta))$$

is an embedding. Let us denote by R the image of this embedding. We have

$$R := \Lambda/\eta\Lambda = \Lambda \otimes \mathbf{Z}_p/\eta\Lambda \otimes \mathbf{Z}_p \subset \mathrm{End}_{\mathbf{F}_p}(J^{(f,p)}(\eta)).$$

Clearly, R contains the identity endomorphism and is stable under the conjugation via Galois automorphisms. Since the $\mathrm{Gal}(K)$-module $J^{(f,p)}(\eta)$ is very simple, either $R = \mathbf{F}_p \cdot \mathrm{Id}$ or $R = \mathrm{End}_{\mathbf{F}_p}(J^{(f,p)}(\eta))$. If $\Lambda/\eta\Lambda = R = \mathbf{F}_p \cdot \mathrm{Id}$ then Λ coincides with $\mathbf{Z}[\delta_p]$. This means that $\mathbf{Z}[\delta_p]$ coincides with its own centralizer in $\mathrm{End}(J^{(f,p)})$ and therefore $\mathbf{Q}(\delta_p)$ is a maximal commutative subalgebra in $\mathrm{End}^0(J^{(f,p)})$.

If $\Lambda/\eta\Lambda = R = \mathrm{End}_{\mathbf{F}_p}(J^{(f,p)}(\eta))$ then, by Nakayama's Lemma,

$$\Lambda \otimes \mathbf{Z}_p = \mathrm{End}_{\mathbf{Z}_p[\delta_p]} T_p(J^{(f,p)}) \cong \mathrm{Mat}_{\frac{2g}{p-1}}(\mathbf{Z}_p[\delta_p]).$$

This implies easily that the $\mathbf{Q}(\delta_p)$-algebra $\Lambda_{\mathbf{Q}} = \Lambda \otimes \mathbf{Q} \subset \mathrm{End}^0(X)$ has dimension $(\frac{2g}{p-1})^2$ and its center has dimension 1. This means that $\Lambda_{\mathbf{Q}}$ is a central $\mathbf{Q}(\delta_p)$-algebra of dimension $(\frac{2g}{p-1})^2$. Clearly, $\Lambda_{\mathbf{Q}}$ coincides with the centralizer of $\mathbf{Q}(\delta_p)$ in $\mathrm{End}^0(J^{(f,p)})$. Since δ_p respects the theta divisor on the jacobian $J^{(f,p)}$, the algebra $\Lambda_{\mathbf{Q}}$ is stable under the corresponding Rosati involution and therefore is semisimple as a $\mathbf{Q}$-algebra. Since its center is the field $\mathbf{Q}(\delta_p)$, the $\mathbf{Q}(\delta_p)$-algebra $\Lambda_{\mathbf{Q}}$ is central simple and has dimension $(\frac{2g}{p-1})^2$. By Theorem 3.6, this cannot happen. Therefore $\mathbf{Q}(\delta_p)$ is a maximal commutative subalgebra in $\mathrm{End}^0(J^{(f,p)})$. □

Proof of main results. Clearly, Theorem 1.1 follows readily from Corollary 5.3. Theorem 1.2 follows readily from Corollary 5.3 combined with Remark 3.9.

References

[1] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson, Atlas of finite groups. Clarendon Press, Oxford, 1985.

[2] Ch. W. Curtis, I. Reiner, Representation theory of finite groups and associative algebras. Interscience Publishers, New York London 1962.

[3] H. K. Farahat, *On the natural representation of the symmetric group*. Proc. Glasgow Math. Association **5** (1961-62), 121–136.

[4] I. M. Isaacs, Character theory of finite groups. Academic Press, New York San Francisco London, 1976.

[5] Ch. Jansen, K. Lux, R. Parker, R. Wilson, An Atlas of Brauer characters. Clarendon Press, Oxford, 1995.

[6] J. K. Koo, *On holomorphic differentials of some algebraic function field of one variable over* C. Bull. Austral. Math. Soc. **43** (1991), 399–405.

[7] B. Moonen, Yu. G. Zarhin, *Hodge and Tate classes on simple abelian fourfolds*. Duke Math. J. **77** (1995), 553–581.

[8] B. Moonen, Yu. G. Zarhin, *Weil classes on abelian varieties*. J. reine angew. Math. **496** (1998), 83–92.

[9] D. Mumford, Abelian varieties, Second edition. Oxford University Press, London, 1974.

[10] K. Ribet, *Galois action on division points of Abelian varieties with real multiplications*. Amer. J. Math. 98 (1976), 751–804.

[11] K. Ribet, *Hodge classes on certain abelian varieties*. Amer. J. Math. **105** (1983), 523–538.

[12] D. Passman, Permutation groups. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[13] B. Poonen, E. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*. J. reine angew. Math. **488** (1997), 141–188.

[14] E. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*. Math. Ann. **310** (1998), 447–471.

[15] J.-P. Serre, Topics in Galois Theory. Jones and Bartlett Publishers, Boston-London, 1992. 163–176;

[16] J.-P. Serre, Linear representations of finite groups. Springer-Verlag, 1977.

[17] M. Suzuki, Group Theory I. Springer-Verlag, 1982.

[18] C. Towse, *Weierstrass points on cyclic covers of the projective line*. Trans. AMS **348** (1996), 3355-3377.

[19] A. Wagner, *The faithful linear representations of least degree of* $\mathbf{S}_n$ *and* $\mathbf{A}_n$ *over a field of odd characteristic*. Math. Z. **154** (1977), 103–114.

[20] Yu. G. Zarhin, *Hyperelliptic jacobians without complex multiplication*. Math. Res. Letters **6**(2000), 123–132.

[21] Yu. G. Zarhin, *Hyperelliptic jacobians and modular representations*, http://xxx.lanl.gov/abs/math.AG/0003002, to appear in "Moduli of abelian varieties" (C. Faber, G. van der Geer, F. Oort, eds.), Birkhäuser.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA

E-mail address: zarhin@math.psu.edu